IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

DARLENE M. KENNEDY, individually and on behalf of all others similarly situated, Plaintiff, v. **GENWORTH FINANCIAL, INC.,** Defendant.	Case No. 3:23cv622 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff Darlene M. Kennedy ("Plaintiff") brings this Class Action Complaint, individually and on behalf of all others similarly situated (the "Class Members"), against Genworth Financial, Inc. ("Defendant" or "Genworth") alleging as follows, based upon information and belief, investigation of counsel, and personal knowledge of Plaintiff.

NATURE OF CASE

1. This class action arises out of the recent targeted cyberattack and data breach where unauthorized third-party criminals retrieved and exfiltrated the highly-sensitive consumer data[1] of Plaintiff, and 2.5-2.7 million Class Members collected by Defendant, via a security vulnerability in a software program used by a third-party vendor contracted by Defendant ("Data Breach").[2] After learning of the Data Breach, Defendant waited over one month to notify affected individuals.[3]

[1] *See* Data Breach Notice, Exhibit A.
[2] U.S. Department of Health and Human Services Cases, Currently Under Investigation, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Aug. 23, 2023).
[3] *Compare* Data Breach Notice dated July 21, 2023, *to CONSUMER ALERT: Data Breach of*

2. Defendant is a "pioneer" in the long term care insurance industry, "helping our customers navigate caregiving options, protect and grow their retirement income, and prepare for the financial challenges that come as we age."[4] As part of its business, Defendant collects the data of its customers and insurance agents, including full names, Social Security numbers, full addresses, policy information, credit and payment data, income or assets, and medical or health data.[5]

3. According to Defendant, information compromised in the Data Breach includes personally identifying information ("PII") of Defendant's customers and insurance agents, such as: Social Security number, first and last name, date of birth, zip code, state of residence, policy number, the role of the individual (ex. Annuitant, Joint Insured, Owner, etc.), product type, and if deceased, the city and date of death, along with the source of that information ("Private Information").[6]

4. Defendant's Privacy Policy, posted on its website, informs consumers that "to protect your personal data":

> We maintain physical, electronic and procedural safeguards. We review these safeguards regularly in keeping with technological advancements. We restrict access to your personal data. We also train our employees in the proper handling of your personal data.[7]

Genworth Third-Party Vendor, Delaware News, https://news.delaware.gov/2023/06/26/consumer-alert-data-breach-of-genworth-third-party-vendor/, announcing June 16, 2023 disclosure by Glenworth of data breach (last accessed Sept. 27, 2023).

[4] *Our Promise*, Genworth, https://www.genworth.com/about-us.html (last accessed Sept. 27, 2023).

[5] *Genworth Privacy Policy*, Genworth, https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf (last accessed Sept. 27, 2023).

[6] *MOVEit Security Event*, Genworth, https://www.genworth.com/moveit.html (last accessed Sept. 27, 2023).

[7] *Genworth Privacy Policy*, Genworth, https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf (last accessed Sept. 27, 2023).

Defendant's Privacy Policy ensures consumers: "We are committed to protecting the personal data we obtain about you."[8]

5. Defendant extends these same assurances to the third-party service providers it contracts with, warranting:

> We require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated.[9]

6. Despite these assurances, Defendant failed to adequately safeguard Plaintiff's and Class Members' highly sensitive Private Information that Defendant collected and maintained. Specifically, a third-party vendor contracted by Defendant, Pension Benefit Information, LLC d/b/a PBI Research Services ("PBI"), used Progress Software Corporation's MOVEit software to transfer the Private Information of Plaintiff and Class Members, and this Private Information was compromised as a result of a security vulnerability in the MOVEit software.

7. It is reported that the Data Breach was carried out by notorious Russia-linked ransomware syndicate Cl0p.[10]

8. Based on the notice posted on Defendant's website, Defendant admits that Plaintiff's and Class Members' Private Information was accessed and compromised by an unauthorized third party.

9. Defendant owed a non-delegable duty to Plaintiff and Class Members to implement

---

[8] *Id.*

[9] *Genworth Online Privacy Policy*, Genworth, https://www.genworth.com/online-privacy-policy.html (last accessed Sept. 27, 2023).

[10] E.g. *Cl0p dumps all MOVEit victim data on clearnet, threat insiders talk ransom strategy*, cybernews (Aug. 18, 2023), https://cybernews.com/security/clop-publish-all-moveit-victim-ransom-data-clearweb/.

reasonable and adequate security measures to protect their Private Information. Yet, Defendant maintained and shared the Private Information in a negligent and/or reckless manner. In particular, Defendant shared the Private Information with a third-party vendor in a condition vulnerable to cyberattacks, and the Private Information was maintained on computer systems in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to ensure its vendors properly safeguarded Plaintiff's and Class Members' Private Information from those risks left that Private Information in a vulnerable condition.

10. Plaintiff's and Class Members' Private Information was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to reasonably and adequately protect Plaintiff's and Class Members' Private Information.

11. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including opening new financial accounts and taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' Private Information to target other phishing and hacking intrusions, using Class Members' information to obtain government benefits, and filing fraudulent tax returns using Class Members' information.

12. As a result of the Data Breach, Plaintiff and Class Members face a substantial risk of imminent and certainly impending harm, heightened here by the loss of Social Security numbers, a class of Private Information which is particularly valuable to identity thieves. Plaintiff and Class Members have and will continue to suffer injuries associated with this risk, including but not limited to a loss of time, mitigation expenses, and anxiety over the misuse of their Private

Information.

13. Even those Class Members who have yet to experience identity theft have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred, and will continue to incur, damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminished value of Private Information, loss of privacy, and/or additional damages as described below.

14. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct and asserting claims for: (i) negligence; (ii) breach of implied contract; (iii) unjust enrichment; (iv) bailment; and (v) breach of fiduciary duty. Through these claims, Plaintiff seeks damages in an amount to be proven at trial, as well as injunctive and other equitable relief, including improvements to Defendant's data security systems, policies, and practices, future annual audits, and adequate credit monitoring services funded by Defendant.

THE PARTIES

15. Plaintiff Darlene M. Kennedy is a natural person, resident, and citizen of the State of Illinois.

16. Defendant obtained and continues to maintain the Private Information of Plaintiff and owed her a legal duty and obligation to protect her Private Information from unauthorized access and disclosure. Plaintiff's Private Information was compromised and disclosed as a result of Defendant's inadequate data security practices, which resulted in the Data Breach.

17. Plaintiff recalls receiving a notice letter dated July 21, 2023 from Defendant's third-party vendor, PBI, stating that an unauthorized party downloaded Plaintiff's Private

Information which she had previously provided to Defendant Genworth.

18. Defendant Genworth Financial, Inc. is a for-profit corporation incorporated in Delaware with its headquarters in Richmond, Virginia. Defendant's principal place of business is located at 6620 West Broad Street Richmond, VA 23230.

JURISDICTION AND VENUE

19. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2) because Plaintiff and at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, there are more than 100 putative class members, and the amount in controversy exceeds $5 million exclusive of interest and costs.

20. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal places of business in Richmond, Virginia, regularly conducts business in Maryland, and has sufficient minimum contacts in Maryland.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant's principal place of business is in this District and a substantial part of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

DEFENDANT'S BUSINESS

22. Defendant is "a Fortune 500 company focused on empowering families to navigate the aging journey with confidence, now and in the future" and "provides guidance, products, and services that help people understand their caregiving options and fund their long-term care needs"[11]

[11] *Company Information*, Genworth, https://investor.genworth.com/company-information (last accessed Sept. 27, 2023).

23. Defendant's core business involves providing a wide range of mortgage, long-term care insurance, life insurance, and other financial products.[12]

24. Defendant's Privacy Policy, accessible on its website, acknowledges that, as part of its ordinary course of business, it collects and stores the Private Information of consumers, such as Plaintiff and Class Members. "We may collect your personal data to provide you with the products or services you requested."[13]

25. Defendant's Privacy Policy acknowledges that Defendant "compl[ies] with Federal and State requirements related to the protection and use of your data."[14]

26. To obtain financial and/or insurance services and products from Defendant, Plaintiff and Class Members must provide Defendant with sensitive Private Information. Defendant may receive this Private Information directly from Plaintiff and Class Members, or from outside parties such as health providers or consumer reporting agencies.[15] As part of its business, Defendant then compiles, stores, and maintains the Private Information it receives from consumers and insurance agents who utilize its services. In Defendant's over 40 years of experience, Defendant has served millions of consumers, indicating that Defendant has created and maintains a massive repository of Private Information, creating a particularly lucrative target for data thieves looking to obtain, misuse, or sell patient data.

27. On information and belief, in the ordinary course of their businesses of providing

[12] 2022 Annual Report: Genworth Financial Inc., Genworth https://d1io3yog0oux5.cloudfront.net/_043938fbccb06c14f97da1f0eb7c06de/genworth/db/2301/22834/annual_report/Genworth--2022+Annual+Report+%28Final%29.pdf.
[13] *Genworth Privacy Policy*, Genworth, https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf (last accessed Sept. 27, 2023).
[14] *Id.*
[15] *Id.*

medical care and services, Defendant maintains the Private Information of consumers, including but not limited to:

- Name, address, phone number and email address;
- Date of birth;
- Demographic information;
- Social Security number or taxpayer identification number;
- Financial and/or payment information;
- Income and assets;
- Accounts at other institutions; and
- Other information that Defendant may deem necessary to provide services and products.

28. Because of the highly sensitive and personal nature of the information Defendant acquires and stores with respect to consumers and other individuals, Defendant, upon information and belief, promises to, among other things: keep Private Information private; comply with financial services industry standards related to data security and Private Information, including FTC guidelines; inform consumers of its legal duties and comply with all federal and state laws protecting consumer Private Information; only use and release Private Information for reasons that relate to the products and services Plaintiff and Class Members obtain from Defendant; and provide adequate notice to individuals if their Private Information is disclosed without authorization.

29. Defendant acknowledges and reiterates these promises in numerous places on its website. For example, Defendant's "Fraud & Information Protection" webpage boasts that "Working to protect your personal information is one of our promises that enables us to help

millions of policyholders secure their financial lives, families, and futures."[16] Defendant's Online Privacy Policy ensures that "Protecting the privacy and security of your personal information is very important to us."[17] Defendant's general Privacy Policy claims: "Our privacy philosophy reflects the value of your trust. We are committed to protecting the personal data we obtain about you."[18] Defendant even promises that third parties contracted by Defendant will live up to these same data security standards: "We require that service providers who have access to your personal information implement similar standards. We require service providers to agree to keep your personal information confidential. Service providers who violate our privacy terms are subject to having their contract terminated."[19]

30. Based on the foregoing, Defendant was aware that it owed non-delegable duties to Plaintiff and Class Members to ensure that their Private Information was safeguarded and to ensure that Defendant had reasonable and adequate security measures, policies, and practices in place to ensure that third parties contracted by Defendant and entrusted with this Private Information by Defendant, would safeguard this Private Information.

31. Yet, contrary to Defendant's representations, Defendant failed to implement adequate data security measures, as evidenced by Defendant's admission of the Data Breach, which affected over 2.5 million customers and agents of Defendant.

THE DATA BREACH AND NOTICE LETTER

[16] *Fraud & Information Protection*, Genworth, https://www.genworth.com/fraud-and-information-protection.html (last accessed Sept. 27, 2023).
[17] *Genworth Online Privacy Policy*, Genworth, https://www.genworth.com/online-privacy-policy.html (last accessed Sept. 27, 2023).
[18] *Genworth Privacy Policy*, Genworth, https://pro.genworth.com/riiproweb/productinfo/pdf/45242.pdf (last accessed Sept. 27, 2023).
[19] *Genworth Online Privacy Policy*, Genworth, https://www.genworth.com/online-privacy-policy.html (last accessed Sept. 27, 2023).

32. According to the Notice Letter, Defendant provided to Plaintiff and Class Members (either via Defendant directly or via Defendant's third-party vendor, PBI), Private Information collected by Defendant was compromised in a cybersecurity attack where unauthorized parties accessed that Private Information between May 29 and May 30, 2023.[20]

33. According to the Notice Letter, On May 31, 2023, Progress Software, the provider of MOVEit Transfer software disclosed a vulnerability in their software that been exploited by an unauthorized third party."[21] Because PBI uses MOVEit in the regular course of its business, PBI "promptly launched an investigation into the nature and scope of the MOVEit vulnerability's impact on our system."[22]

34. Through PBI's investigation, PBI determined that an unauthorized "third party accessed one of our MOVEit Transfer Servers on May 29, 2023 and May 30, 2023 and downloaded [Plaintiff's and Class Members'] data."[23]

35. According to the Notice Letter, the types of information exfiltrated in the Data Breach included individuals' "name, Social Security number, date of birth, zip code, state of residence, role in policy/account (eg., Annuitant, Joint Insured, Owner, etc.), general product type, and policy/account number."[24] Defendant's website additionally notes for customers, if deceased, "the exposed information also includes the city and date of death, along with the source of that information."[25] For impacted agents, Defendant's website reports that the information exposed in

[20] *See* Notice Letter.
[21] *Id.*
[22] *id.*
[23] *See id.*
[24] *See id.*
[25] *MOVEit Security Event*, Genworth, https://www.genworth.com/moveit.html (last accessed Sept. 27, 2023).

the Data Breach includes: "social security number, first and last name, date of birth, full address, and a preferred full address" and, if deceased, the "date of death and the source of that information."[26]

36. On June 16, 2023, PBI reportedly advised Genworth that "specific Genworth files containing policyholder and agent information were compromised" in the Data Breach.[27] Yet, Genworth waited over one month to begin sending Notice Letters to affected individuals, with certain Class Members, including Plaintiff, never receiving a notice directly from Genworth, the entity to which they entrusted their Private Information. Rather, Plaintiff and other Class Members learned of the Data Breach only from PBI. This slow and/or absent response occurred, despite Defendant's 2022 Annual Report acknowledging that "an increasing number of states and foreign countries require that affected parties be notified or other actions be taken (which could involve significant costs to us) if a security breach results in the unlawful disclosure of personal information," as occurred here.[28]

37. In the aftermath of the Data Breach, Defendant claims that it is "making sure this doesn't happen again" by doing the following:

> We have implemented technical, physical, and process safeguards to maintain the confidentiality of customer information. Further, we require third parties that receive and store the personal information of our customers to take similar steps, and we work to understand the measures they have taken. While the MOVEit event has impacted various organizations globally, Genworth will continue to focus on and seek opportunities to improve how third parties protect the data of our customers.[29]

---

[26] *Id.*
[27] *MOVEit Security Event*, Genworth, https://www.genworth.com/moveit.html (last accessed Sept. 27, 2023).
[28] https://www.hopkinsmedicine.org/Privacy/_docs/notice-of-privacy-practices-providers.pdf.
[29] *MOVEit Security Event*, Genworth, https://www.genworth.com/moveit.html (last accessed Sept. 27, 2023).

However, there is no indication whether these measures are adequate to protect Plaintiff's and Class Members' Private Information going forward.

38. Defendant's accessed data contained Private Information that was accessible, unencrypted, unprotected, and vulnerable for acquisition and/or exfiltration by the unauthorized actor which Defendant electively shared with its third-party vendor, PBI.

39. As a financial entity that collects, creates, maintains, and shares/transfers significant volumes of Private Information, the targeted attack was a foreseeable risk which Defendant was aware of and knew it had a duty to guard against. It is well-known that insurance and financial services providers such as Defendant, which collect and store the confidential and sensitive Private Information of millions of individuals, and the third-party vendors with which these entitles share that information, are frequently targeted by cyberattacks. Further, cyberattacks are highly preventable through the implementation of reasonable and adequate cybersecurity safeguards, including proper oversight of the cybersecurity practices of third-party vendors and reasonable and adequate data sharing practices and policies.

40. The targeted cyberattack was expressly designed to gain access to and exfiltrate private and confidential data, including (among other things) the Private Information of consumers, like Plaintiff and Class Members.

41. Defendant had obligations created by federal and state regulations, contract, industry standards, common law, and its own promises and representations made to Plaintiff and Class Members to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

42. Plaintiff and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its

obligations to keep such information confidential and secure from unauthorized access.

43. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew, or should have known, that they were responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure.

44. Due to Defendant's inadequate security policies and practices and its delayed notice to victims, Plaintiff and Class Members now face a present, immediate, and ongoing risk of fraud and identity theft that they will have to deal with for the rest of their lives.

45. Defendant shared Plaintiff's and Class Members' Private Information with a third-party vendor, PBI, and according to published reports, PBI fell victim to a MOVEit Transfer attack, carried out by Russia-linked ransomware syndicate Cl0p.

46. MOVEit Transfer is a managed file transfer software. The zero-day bug affected MOVEit Transfer's servers, allowing attackers to access and download the data stored there, including that of Defendant.

47. Cl0p posted on their dark web blog that they had taken Defendant's data.

48. The Cl0p ransomware gang has taken credit for exploiting the MOVEit zero-day bug. They claim to have breached hundreds of companies in the process.

49. So far, over 200 organizations have fallen victim to the MOVEit attacks, with the estimated number of exposed people exceeding 17 million. Cl0p has been posting victims' names on their dark web leak site since June 14, 2023. The extent of the exposed data depends on how a certain company uses the file transfer system.

50. Cl0p operates under the Ransomware-as-a-Service (RaaS) mode, which means that it rents the software to affiliates for a pre-agreed cut of the ransom payment.

51. Cl0p employs the "double-extortion" technique of stealing and encrypting victim data, refusing to restore access, and publishing exfiltrated data into its data leak site if the ransom is not paid. On information and belief, neither Defendant nor PBI paid a ransom to Cl0p.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice

52. As a financial services entity entrusted with the highly sensitive Private Information of consumers, federal and state regulations require Defendant to implement adequate safeguards to prevent unauthorized use or disclosure of Private Information. Defendant, itself acknowledges, in its 2022 Annual Report to Shareholders that:

> In the United States, federal and state laws and regulations require financial institutions, including insurance companies, to protect the security and privacy of consumer financial information and to notify consumers about policies and practices relating to the collection, use and disclosure of consumer information, as well as policies relating to protecting the confidentiality, integrity and availability of that information.[30]

53. In Defendant's 2023 Proxy Statement, Defendant includes a "Spotlight on Cybersecurity Risk," in which it further acknowledges the vital importance of maintaining adequate and reasonable security measures:

> Genworth recognizes the significant operational risk, including risk of losses, from cyberattacks and the importance of a strong cybersecurity program for effective risk management. Our Board recognizes the importance of maintaining the privacy and security of customer information, as well as the availability of our systems and consequently dedicates meaningful time and attention to oversight of cybersecurity risk. In light of these risks, our Board is actively engaged in the oversight of our Company's Information Security and Information Technology ("IT") Risk Program, which includes periodic briefings on cybersecurity threats and participation in cybersecurity preparedness exercises.[31]

---

[30] 2022 Annual Report: Genworth Financial Inc., Genworth https://d1io3yog0oux5.cloudfront.net/_043938fbccb06c14f97da1f0eb7c06de/genworth/db/2301/22834/annual_report/Genworth--2022+Annual+Report+%28Final%29.pdf.

[31] Notice of 2023 Annual Meeting and Proxy Statement: Genworth Financial, Inc., Genworth, https://d1io3yog0oux5.cloudfront.net/_043938fbccb06c14f97da1f0eb7c06de/genworth/db/2301/22834/proxy_statement_pdf/Genworth--

54. Additionally, Defendant explicitly recognizes the heightened standards of security necessary to ensure the protection of Private Information in recent years:

> The area of cybersecurity and data privacy have come under increased scrutiny in recent years, with various countries, government agencies and insurance regulators introducing and/or passing legislation in an attempt to safeguard personal information from escalating cybersecurity threats. For additional details, see "Regulation— Other Laws and Regulations—Cybersecurity" and "Regulation—Other Laws and Regulations—Privacy of Consumer Information."[32]

Defendant claims to "have implemented internal policies, practices and controls designed to comply with applicable data privacy and security laws."[33]

55. However, Defendant did not maintain adequate security to protect the Private Information it collected from infiltration by cybercriminals, and Defendant waited over one month to notify affected individuals of the Data Breach.

56. More specifically, Defendant explicitly acknowledges that the nature of the information it collected and maintained from Plaintiff and Class Members made it uniquely susceptible to cyberattacks that could compromise consumer's Private Information:

> We retain confidential information in our computer systems, and we rely on commercial technologies to maintain the security of those systems, including computers or mobile devices. *Anyone who is able to circumvent our security measures and penetrate our computer systems or misuse authorized access could access, view, misappropriate, alter, delete or disclose any information in the systems, including personal information, personal health information and proprietary business information*.[34]

2023%2BProxy%2BStatement%2B%2528Final%2529.pdf.

[32] 2022 Annual Report: Genworth Financial Inc., Genworth https://d1io3yog0oux5.cloudfront.net/_043938fbccb06c14f97da1f0eb7c06de/genworth/db/2301/22834/annual_report/Genworth--2022+Annual+Report+%28Final%29.pdf.

[33] *Id.*

[34] *Id.* (emphasis added).

57. Defendant also should have been on heightened notice of the risk of possible cyberattacks, such as the one which compromised Plaintiff's and Class Members' Private Information, because it has been the target of such attacks in the past. "We have experienced occasional, actual or attempted breaches of our cybersecurity, although to date, none of these breaches has had a material effect on our business, operations or reputation."[35]

58. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure, including disclosure resulting from a breach of a third-party vendor with whom Defendant shares consumers' Private Information. Defendant acknowledges as much in its 2022 Annual Shareholder Report:

> Any compromise of the security of our computer systems or those of our partners and third-party service providers that results in the unauthorized disclosure of customer personal information could damage our reputation in the marketplace, deter people from purchasing our products, subject us to significant civil and criminal liability and require us to incur significant technical, legal and other expenses.[36]

59. Based on the foregoing, Defendant knew that it owed Plaintiff and Class Members non-delegable duties to keep the Private Information it collected, maintained, and/or transferred to and shared with selected third-parties, secure and protected. Defendant's duty, as Defendant itself acknowledges, extended to the third parties, like PBI, with which Defendant shared this Private Information; Defendant was required to ensure these third parties implemented reasonable and adequate security measures necessary to secure Plaintiff's and Class Members' Private

[35] *Id.*
[36] *Id.*

Information.

60. As described throughout this Complaint, Defendant did not implement reasonable security practices and policies to protect Plaintiff's and Class Members' Private Information prior to, during, or after the Data Breach, but rather, enacted unreasonable data security measures and failed to ensure that Defendant's third-party vendors which it elected to share this Private Information with had reasonable data security measures, which it knew or should have known were insufficient to reasonably protect the highly sensitive information Defendant collected. Consequently, cybercriminals circumvented the security measures of a vendor Defendant elected to contract with and share Plaintiff's and Class Members' data with, resulting in a significant Data Breach.

Defendant Fails to Comply with FTC Guidelines

61. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should factor into all business decision-making.

62. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[37] The guidelines also recommend that businesses use an intrusion detection

[37] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (Oct. 2016), *available at* https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and, have a response plan ready in the event of a breach.[38]

63. The FTC further recommends that companies not maintain PII longer than necessary for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

64. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

65. These FTC enforcement actions include actions against financial services providers and partners like Defendant.

66. Genworth failed to properly implement basic data security practices and oversight.

67. Genworth's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' Private Information which it collected and electively shared with third-party vendors constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

[38] *Id*.

68. Genworth was at all times fully aware of its obligation to protect the Private Information of customers and insurance agents. Genworth was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

69. As shown above, experts studying cybersecurity routinely identify financial services providers and partners as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

70. Several best practices have been identified that at a minimum should be implemented by financial service providers like Defendant, including but not limited to; educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key, multi-factor authentication, backup data, and limiting which employees can access sensitive data.

71. Other best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

72. On information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established

standards for reasonable cybersecurity readiness.

73. These foregoing frameworks are existing and applicable industry standards in the financial services industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft

74. Cyberattacks and data breaches at financial services providers like Defendant are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

75. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft face "substantial costs and time to repair the damage to their good name and credit record."[39]

76. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal PII is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security

[39] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), *available at* https://www.gao.gov/new.items/d07737.pdf.

number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

77. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[40]

78. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

79. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

80. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.[41]

---

[40] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Aug. 24, 2023).

[41] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech.

81. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

82. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

83. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

84. Private Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

85. Thus, Plaintiff and Class Members must vigilantly monitor their financial and medical accounts, or the accounts of deceased individuals for whom Class Members are the executors or surviving spouses, for many years to come.

86. Private Information can sell for as much as $363 per record according to the Infosec

---

11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

Institute.[42] Private Information is particularly valuable because criminals can use it to target victims with frauds and scams. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

87. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[43] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[44] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

88. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

89. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[45]

---

[42] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.
[43] *Identity Theft and Your Social Security Number*, Social Security Administration (July 2021), *available at* https://www.ssa.gov/pubs/EN-05-10064.pdf.
[44] *Id*.
[45] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

90. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[46]

91. Because of the value of its collected and stored data, the financial services industry has experienced disproportionally higher numbers of data theft events than other industries.

92. For this reason, Defendant knew or should have known about these dangers and strengthened their data and email handling systems accordingly. Defendant was on notice of the substantial and foreseeable risk of harm from a data breach, yet Defendant failed to properly prepare for that risk.

DEFENDANT'S DATA BREACH

93. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data, and the systems of third parties with which Defendant voluntarily shared Plaintiff's and Class Members' Private Information. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to ensure that its vendors with access to its computer systems and

[46] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

data employed reasonable security procedures;

d. Failing to ensure the confidentiality and integrity of electronic PII they created, received, maintained, and/or transmitted,

e. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

g. Failing to adhere to industry standards for cybersecurity as discussed above; and

h. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

94. Genworth negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access Genworth computer network and systems for multiple days which contained unsecured and unencrypted Private Information.

95. Accordingly, as outlined below, Plaintiff and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiff and the Class Members also lost the benefit of the bargain they made with Defendant.

Plaintiff's and Class Members' Damages

96. Given the sensitivity of the Private Information involved in this Data Breach, Plaintiff and Class Members have all suffered damages and will face a substantial risk of additional injuries for years to come, if not the rest of their lives. Defendant has done nothing to compensate Plaintiff or Class Members for many of the injuries they have already suffered. Defendant has not

demonstrated any efforts to prevent additional harm from befalling Plaintiff and Class Members as a result of the Data Breach.

97. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

98. Plaintiff's and Class Members' demographic information, dates of birth, and Social Security Numbers were all compromised in the Data Breach and are now in the hands of the cybercriminals.

99. Since being notified of the Data Breach, Plaintiff has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

100. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, cancelling credit and debit cards, and monitoring her accounts for fraudulent activity.

101. Plaintiff's and Class Members' Private Information was compromised as a direct and proximate result of the Data Breach.

102. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

103. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to spend time dealing with the effects of the Data Breach.

104. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills

opened in their names, credit card fraud, and similar identity theft.

105. Indeed, Plaintiff has already suffered harms from the theft of her identity, whereupon an identity thief was able to satisfactorily impersonate plaintiff to withdraw $4,000 from Plaintiff's bank account, as discussed in greater detail below.

106. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on Plaintiff's and Class Members' Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

107. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

108. Plaintiff and Class Members also suffered a loss of value of their Private Information when they were acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

109. Plaintiff and Class Members were also damaged via benefit-of-the-bargain damages. Plaintiff and Class Members overpaid for a service that was intended to be accompanied by adequate data security that complied with industry standards but was not. Part of the price Plaintiff and Class Members paid to Defendant and/or Defendant's third-party vendors was intended to be used by Defendant to fund adequate security of their computer system(s) and Plaintiff's and Class Members' Private Information. Thus, Plaintiff and Class Members did not get what they paid for and agreed to.

110. Plaintiff and Class Members have spent and will continue to spend significant amounts of time monitoring their accounts and sensitive information for misuse.

111. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and

f. Closely reviewing and monitoring Social Security Numbers, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

112. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected, and that Defendant reasonably and adequately oversees the data security measures implemented by third-parties with which Defendant shares Plaintiff's and Class Members' sensitive Private Information.

113. Further, as a result of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

114. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, loss of time, loss of privacy, and are at an increased risk of future harm.

Plaintiff's Experience

115. Plaintiff provided her Private Information to Genworth directly when she obtained financial services from Genworth in the form of a term life insurance policy.

116. According to the Data Breach Notice Letter Plaintiff received, Plaintiff's personal information was involved in the Data Breach.[47]

117. Upon information and belief, Plaintiff was presented with standard forms to complete prior to receiving financial services that required her to provide Genworth with her PII. Upon information and belief, Defendant received and maintains the information Plaintiff was required to provide.

118. Plaintiff is very careful with her Private Information. She stores any documents containing her Private Information in a safe and secure location or destroys the documents. Plaintiff has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff diligently chooses unique usernames and passwords for her various online accounts.

119. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the

[47] *See Notice Letter*.

impact of the Data Breach after receiving the data breach notification letter, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, and monitoring her credit.

120. Plaintiff was forced to spend multiple hours attempting to mitigate the effects of the Data Breach. She will continue to spend valuable time she otherwise would have spent on other activities, including but not limited to work and/or recreation. This is time that is lost forever and cannot be recaptured.

121. However, despite these best efforts to mitigate the impact of the Data Breach, Plaintiff still fell victim to identity theft, when an individual came into her local bank in Charlotte, North Carolina and successfully withdrew funds in the amount of $4,000 using Plaintiff's stolen identity information. Despite the bank teller's best attempts to validate the identity of the identity thief by conducting an extensive interview, the identity thief was still able to satisfactorily answer these questions using Plaintiff's stolen identity information, whereupon the money was turned over and the thief left the bank.

122. Plaintiff suffered actual injury and damages from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) the loss of $4,000 due to identity theft; (b) diminution in the value of her Private Information, a form of intangible property that Genworth obtained from Plaintiff; (c) violation of her privacy rights; (d) the theft of her Private Information; (e) loss of time; (f) imminent and impending injury arising from the increased risk of identity theft and fraud, including the loss of $4,000 misappropriated from her bank account; (g) failure to receive the benefit of her bargain; and (h) nominal and statutory damages.

123. Plaintiff has also suffered emotional distress that is proportional to the risk of harm

and loss of privacy caused by the theft of her Private Information, which she believed would be protected from unauthorized access and disclosure, including anxiety about unauthorized parties viewing, selling, and/or using her Private Information for purposes of identity theft and fraud. Plaintiff has also suffered anxiety about unauthorized parties viewing, using, and/or publishing information related to her Social Security number and insurance policy.

124. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud in perpetuity.

125. Plaintiff has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

126. Plaintiff brings this action against Defendant individually and on behalf of all other persons similarly situated ("the Class").

127. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons or, if minors, their parents or guardians, or, if deceased, their executors or surviving spouses, who Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

128. Excluded from the Class are Defendant's officers, directors, and employees; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members

of the judiciary to whom this case is assigned, their families and Members of their staff.

129. Plaintiff reserves the right to amend or modify the Class definition or create additional subclasses as this case progresses.

130. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. Genworth reports that 2.5-2.7 million individuals were impacted by the data breach.[48]

131. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security practices and policies prior to and during the Data Breach complied with applicable data security laws and regulations, including in its oversight of third parties with which Defendant shared sensitive Private Information;

d. Whether Defendant's data security practices and policies prior to and during the Data Breach were consistent with industry standards, including in its oversight of third parties with which Defendant shared sensitive

[48] https://www.genworth.com/moveit.html (last accessed Sept. 27, 2023).

Private Information;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Defendant should have notified Plaintiff and Class Members of the Data Breach sooner;

j. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

k. Whether Defendant's conduct was negligent;

l. Whether Defendant breached implied contracts with Plaintiff and Class Members;

m. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

n. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

o. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, treble damages, and/or injunctive relief.

132. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data

Breach.

133. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel are competent and experienced in litigating class actions.

134. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the data of Plaintiff and Class Members was stored on the same network and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

135. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, to conduct this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

136. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

137. Likewise, particular issues under Rule 42(d)(l) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, transmitting and/or sharing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect Plaintiff's and Class Members' data when sharing it with third parties were reasonable in light of best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures, policies, and practices amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

138. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant or PBI.

CLAIMS FOR RELIEF

COUNT I
Negligence
(*On Behalf of Plaintiff and the Class*)

139. Plaintiff re-alleges and incorporates by reference paragraphs 1–138 as if fully set forth herein.

140. By collecting and storing the Private Information of Plaintiff and Class Members, in their computer system and network, and sharing it and using it for commercial gain, Defendant owed a duty of care to use reasonable means to secure and safeguard Plaintiff's and Class Members' Private Information, to prevent inadvertent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it ensured that the data security systems and practices of third parties with which they shared Plaintiff's and Class Members' Private Information would reasonably and adequately safeguard that Private Information, as well as ensure there were processes to detect a data breach in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

141. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that that the systems and networks which held Plaintiff's and Class Members' Private Information, including the systems of third parties to which Defendant transferred that Private Information, and the personnel responsible for them, adequately protected the Private Information.

142. Plaintiff and Class Members are a well-defined, foreseeable, and probable group of consumers and agents that Defendant was aware, or should have been aware, could be injured by inadequate data security measures.

143. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and consumers, which is recognized by laws and regulations including but not limited to the FTC Act and common law. Defendant was in a superior position to ensure that its systems and the systems of its third-party vendors were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

144. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

145. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information entrusted to it.

146. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of the systems of its third party vendors to which Defendant transferred and/or shared Class Members' Private Information;

c. Failing to have in place mitigation policies and procedures;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private

Information had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

147. Plaintiff and Class Members have no ability to protect their Private Information that was or remains in Defendant's possession or the possession of Defendant's third-party vendors.

148. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the financial services industry.

149. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

150. Defendant's conduct was grossly negligent and departed from reasonable standards of care, including but not limited to, failing to adequately protect the Private Information and failing to provide Plaintiff and Class Members with timely notice that their sensitive Private Information had been compromised.

151. Neither Plaintiff nor Class Members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

152. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *e.g.,* (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

153. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet their duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

154. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

COUNT II
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

155. Plaintiff re-alleges and incorporates by reference paragraphs 1–138 as if fully set forth herein.

156. Defendant acquired and maintained the Private Information of Plaintiff and the Class that they received directly from them.

157. When Plaintiff and Class Members paid money and provided their Private Information to Defendant in exchange for goods or services, they entered into implied contracts with Defendant.

158. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members that their information had been breached and compromised.

159. Plaintiff and the Class were required to deliver their Private Information to Defendant as part of the process of obtaining services provided by Defendant. Plaintiff and Class Members paid money, or money was paid on their behalf, to Defendant in exchange for services.

160. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

161. Defendant accepted possession of Plaintiff's and Class Members' Private Information for the purpose of providing services or Plaintiff and Class Members.

162. In accepting such information and payment for services, Defendant entered into an implied contract with Plaintiff and the other Class Members whereby Defendant became obligated to reasonably safeguard Plaintiff's and the other Class Members' Private Information.

163. Alternatively, Plaintiff and Class Members were the intended beneficiaries of data protection agreements entered into between Defendant and Defendant's third-party vendors.

164. In delivering their Private Information to Defendant and paying for financial services, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard the data as part of that service.

165. The implied promise of confidentiality includes consideration beyond those pre-existing general duties owed under state of federal regulations. The additional consideration included implied promises to take adequate steps to comply with specific industry data security standards and FTC guidelines on data security.

166. The implied promises include but are not limited to: (1) taking steps to ensure that any agents who are granted access to Private Information also protect the confidentiality of that data; (2) taking steps to ensure that the information that is placed in the control of their agents is restricted and limited to achieve an authorized purpose; (3) restricting access to qualified and trained agents; (4) designing and implementing appropriate retention policies to protect the information against criminal data breaches; (5) applying or requiring proper encryption; (6)

multifactor authentication for access; and (7) other steps to protect against foreseeable data breaches.

167. Plaintiff and the Class Members would not have entrusted their Private Information to Defendant in the absence of such an implied contract.

168. Had Defendant disclosed to Plaintiff and the Class that they did not have adequate computer and security practices and policies to secure sensitive data, including data shared with Defendant's third-party vendors, Plaintiff and the other Class Members would not have provided their Private Information to Defendant.

169. Defendant recognized that Plaintiff's and Class Members' Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and the other Class Members.

170. Plaintiff and the other Class Members fully performed their obligations under the implied contracts with Defendant.

171. Defendant breached the implied contract with Plaintiff and the other Class Members by failing to take reasonable measures to safeguard their Private Information as described herein.

172. As a direct and proximate result of Defendant's conduct, Plaintiff and the other Class Members suffered and will continue to suffer damages in an amount to be proven at trial.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

173. Plaintiff re-alleges and incorporates by reference paragraphs 1–1378 as if fully set forth herein.

174. This count is pleaded in the alternative to breach of contract.

175. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including from money it makes based upon protecting Plaintiff's and Class Members' Private Information.

176. There is a direct nexus between money paid to Defendant and the requirement that Defendant keeps Plaintiff's and Class Members' Private Information confidential and protected.

177. Plaintiff and Class Members paid Defendant a certain sum of money, which was used to fund data security via contracts with Defendant.

178. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

179. Protecting data from Plaintiff and Class Members is integral to Defendant's business. Without their data, Defendant would be unable to provide the insurance and financial services comprising Defendant's core business.

180. Plaintiff's and Class Members' data has monetary value. Plaintiff and Class Members directly and indirectly conferred a monetary benefit on Defendant. They indirectly conferred a monetary benefit on Defendant by purchasing goods and/or services from Defendant, and from which Defendant received compensation to protect certain data. Plaintiff and Class Members directly conferred a monetary benefit on Defendant by supplying Private Information, which has value, from which value Defendant derives its business value, and which should have been protected with adequate data security.

181. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

182. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to avoid their data security obligations at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

183. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

184. Defendant acquired the monetary benefit and Private Information through inequitable means in that they failed to disclose the inadequate security practices previously alleged.

185. If Plaintiff and Class Members knew that Defendant had not secured its Private Information, they would not have agreed to provide their Private Information to Defendant.

186. Plaintiff and Class Members have no adequate remedy at law.

187. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity

addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; (vii) loss or privacy from the authorized access and exfiltration of their Private Information; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

188. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

189. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

COUNT IV
Bailment
(*On Behalf of Plaintiff and the Class*)

190. Plaintiff re-alleges and incorporates by reference paragraphs 1–138 as if set fully forth herein.

191. Plaintiff and Class Members provided Private Information to the Defendant, which Defendant was under a duty to keep private and confidential.

192. Plaintiff's and Class Members' Private Information is personal property and was conveyed to Defendant for the certain purpose of keeping the information private and confidential.

193. Plaintiff's and Class Members' Private Information has value and is highly prized by hackers and criminals. Defendant was aware of the risks it took when accepting the Private Information for safeguarding and assumed the risk voluntarily.

194. Once Defendant accepted Plaintiff's and Class Members' Private Information, it was in the exclusive possession of that information, and neither Plaintiff nor Class Members could control that information once they were within the possession, custody, and control of Defendant.

195. Defendant did not safeguard Plaintiff's or Class Members' Private Information when it failed to adopt and enforce adequate security safeguards to prevent a known risk of a cyberattack.

196. Defendant's failure to safeguard Plaintiff's and Class Members' Private Information resulted in that information being accessed or obtained by third-party cybercriminals.

197. As a result of Defendant's failure to keep Plaintiff's and Class Members' Private Information secure, Plaintiff and Class Members suffered injury, for which compensation—including nominal damages and compensatory damages—are appropriate.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiff and the Class)

198. Plaintiff re-alleges and incorporates by reference paragraphs 1–138 as if fully set forth herein.

199. In light of the special relationship between Defendant and Plaintiff and Class Members, Defendant became a fiduciary by undertaking a guardianship of the Private Information to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where)

Defendant does store it.

200. Defendant had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship with its customers and agents, in particular, to keep secure their Private Information.

201. Defendant breached its fiduciary duty to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

202. Defendant breached its fiduciary duty to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

203. As a direct and proximate result of Defendant's breach of its fiduciary duty, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

204. As a direct and proximate result of Defendant's breach of their fiduciary duty,

Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and her counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for not less than five years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, nominal damages, and/or statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) Pre- and post-judgment interest on any amounts awarded; and,

i) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38(b), Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: September 29, 2023

Respectfully submitted,

DARLENE M. KENNEDY, individually and on behalf of all others similarly situated
By Counsel

/s/_____

Bernard J. DiMuro, Esq. (VSB #18784)
DiMuroGinsberg, P.C.
1001 N Fairfax Street, Suite 510
Alexandria, VA 22314
Phone: 703.684.4333
Fax: 703.548.3181
Email: bdimuro@dimuro.com

James J. Pizzirusso*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
(202) 540-7200
jpizzirusso@hausfeld.com

Amanda V. Boltax*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
(202) 849-4140
mboltax@hausfeld.com

Steven M. Nathan*
HAUSFELD LLP
33 Whitehall Street
Fourteenth Floor
New York, NY 10004
(646) 357-1100
snathan@hausfeld.com

Counsel for Plaintiff
** Pro Have Vice Forthcoming*